Biswajit Bhattacharjee (19) & Biswaraj Das Purkayastha (20)

Presents

SECURITY & CONTROL OF INFORMATION SYSTEM

- PRESENTED TO :

Deepjyoti Choudhury

Assistant Professor

Assam University, Silchar

- **Information system:**

The term information system describes the organized collection, processing, transmission, and spreading of information in accordance with defined procedures, whether automated or manual.

- **Security:**

Policies, procedures and technical measures used to prevent unauthorized access, alteration, theft, or physical damage to information systems

- **Controls:**

Methods, policies, and organizational procedures that ensure safety of organization’s assets; accuracy and reliability of its accounting records; and operational adherence to management standards

Basic Principles of Information Systems Security

A . Confidentiality

This principle is applied to information by enforcing rules about who is allowed to know it. Preserving personal privacy is one of the major objectives of confidentiality. It prevents the unauthorized disclosure of information and restricts the data access to only those who are authorized. But today the world is moving towards less authoritative structures, more informality, and fewer rules. Such developments are creating an issue of concern for the principle of confidentiality since the developments are aimed at making information accessible to many, not few.

Basic Principles of Information Systems Security (cont…)

B. Integrity

In any business organization having IS, the values of data stored and manipulated, such as maintaining the correct signs and symbols is an important issue of concern. This issue is referred to integrity within an organization which is the prevention of the unauthorized modification.

C. Availability

Availability is referred to as accessibility of information

and in usable form when and where it is required. Sometimes it is also explained as the prevention of unauthorized withholding of data or resources. Within any organization today availability of resources and data is an important issue of concern since system failure is an organizational security issue

System Vulnerability and Abuse

Why systems are vulnerable

- Accessibility of networks
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, unauthorized changes)
- Disasters
- Use of networks/computers outside of firm's control
- Loss and theft of portable devices

System Vulnerability and Abuse

- Internet vulnerabilities
  - Network open to anyone
  - Size of Internet means abuses can have wide impact
  - Use of fixed Internet addresses with cable or DSL modems creates fixed targets hackers
  - Unencrypted VOIP
  - E-mail, P2P, IM
    - Interception
    - Attachments with malicious software
    - Transmitting trade secrets

System Vulnerability and Abuse

- Wireless security challenges
  - Radio frequency bands easy to scan
  - SSIDs (service set identifiers)
    - Identify access points
    - Broadcast multiple times
    - **War driving**
      - Eavesdroppers drive by buildings and try to detect SSID and gain access to network and resources
  - WEP (Wired Equivalent Privacy)
    - Security standard for 802.11; use is optional
    - Uses shared password for both users and access point
    - Users often fail to implement WEP or stronger systems

System Vulnerability and Abuse

- Malware (malicious software)
  - Viruses
    - Rogue software program that attaches itself to other software programs or data files in order to be executed
  - Worms
    - Independent computer programs that copy themselves from one computer to other computers over a network.
  - Trojan horses
    - Software program that appears to be benign but then does something other than expected.

System Vulnerability and Abuse

- Malware (cont.)
  - SQL injection attacks
    - Hackers submit data to Web forms that exploits site’s unprotected software and sends rogue SQL query to database
  - Spyware
    - Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising
  - Key loggers
    - Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks

System Vulnerability and Abuse

- Hackers and computer crime
  - Hackers vs. crackers
  - Activities include
    - System intrusion
    - System damage
    - Cybervandalism
      - Intentional disruption, defacement, destruction of Web site or corporate information system

System Vulnerability and Abuse

- Spoofing
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Redirecting Web link to address different from intended one, with site masquerading as intended destination

- Sniffer
  - Eavesdropping program that monitors information traveling over network
  - Enables hackers to steal proprietary information such as e-mail, company files, etc.

System Vulnerability and Abuse

- Denial-of-service attacks (DoS)
  - Flooding server with thousands of false requests to crash the network.

- Distributed denial-of-service attacks (DDoS)
  - Use of numerous computers to launch a DoS
  - Botnets
    - Networks of “zombie” PCs infiltrated by bot malware
    - Worldwide, 6 - 24 million computers serve as zombie PCs in thousands of botnets

System Vulnerability and Abuse

- Computer crime
  - Defined as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”
  - Computer may be target of crime, e.g.:
    - Breaching confidentiality of protected computerized data
    - Accessing a computer system without authority
  - Computer may be instrument of crime, e.g.:
    - Theft of trade secrets
    - Using e-mail for threats or harassment

System Vulnerability and Abuse

- Identity theft
  - Theft of personal Information (social security id, driver’s license or credit card numbers) to impersonate someone else
- Phishing
  - Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask users for confidential personal data.
- Evil twins
  - Wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet

System Vulnerability and Abuse

- Pharming
  - Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser
- Click fraud
  - Occurs when individual or computer program fraudulently clicks on online ad without any intention of learning more about the advertiser or making a purchase
- Cyberterrorism and Cyberwarfare

System Vulnerability and Abuse

- Internal threats: employees
  - Security threats often originate inside an organization
  - Inside knowledge
  - Sloppy security procedures
    - User lack of knowledge
  - Social engineering:
    - Tricking employees into revealing their passwords by pretending to be legitimate members of the company in need of information

System Vulnerability and Abuse

- Software vulnerability
  - Commercial software contains flaws that create security vulnerabilities
    - Hidden bugs (program code defects)
      - Zero defects cannot be achieved because complete testing is not possible with large programs
    - Flaws can open networks to intruders
  - Patches
    - Vendors release small pieces of software to repair flaws
    - However exploits often created faster than patches be released and implemented

General Controls and Application Controls

General controls

- Establish framework for controlling design, security, and use of computer programs
- Include software, hardware, computer operations, data security, implementation, and administrative controls

General controls

- Software controls
  - Authorised access to systems
- Hardware controls
  - Physically secure hardware
  - Monitor for and fix malfunction
  - Environmental systems and protection
  - Backup of disk-based data

General controls

- Computer operations controls
  - Day-to-day operations of Information Systems
  - Procedures
  - System set-up
  - Job processing
  - Backup and recovery procedures
- Data security controls
  - Prevent unauthorised access, change or destruction
  - When data is in use or being stored
  - Physical access to terminals
  - Password protection
  - Data level access controls

General controls

- Administrative controls
  - Ensure organisational policies, procedures and standards and enforced
  - Segregation of functions to reduce errors and fraud
  - Supervision of personal to ensure policies and procedures are being adhered to

General Controls and Application Controls

Application controls

- Unique to each computerized application
- Include input, processing, and output controls

Application controls

- Input controls
  - Data is accurate and consistent on entry
  - Direct keying of data, double entry or automated input
  - Data conversion, editing and error handling
  - Field validation on entry
  - Input authorisation and auditing
  - Checks on totals to catch errors

Application controls

- Processing controls
  - Data is accurate and complete on processing
  - Checks on totals to catch errors
  - Compare to master records to catch errors
  - Field validation on update

Application controls

- Output controls
  - Data is accurate, complete and properly distributed on output
  - Checks on totals to catch errors
  - Review processing logs
  - Track recipients of data

Protecting the Digital Firm

- ***On-line transaction processing:*** Transactions entered online are immediately processed by computer

- ***Fault-tolerant computer systems:*** Contain extra hardware, software, and power supply components to provide continuous uninterrupted service

Protecting the Digital Firm

- ***High-availability computing:*** Tools and technologies enabling system to recover quickly from a crash

- ***Disaster recovery plan:*** Runs business in event of computer outage

- ***Load balancing:*** Distributes large number of requests for access among multiple servers

Protecting the Digital Firm

- ***Mirroring:*** Duplicating all processes and transactions of server on backup server to prevent any interruption in service

- ***Clustering:*** Linking two computers together so that a second computer can act as a backup to the primary computer or speed up processing

Internet Security Challenges

Firewalls

- Prevent unauthorized users from accessing private networks
- Two types: proxies and stateful inspection

Intrusion Detection System

- Monitors vulnerable points in network to detect and deter unauthorized intruders

Security and Electronic Commerce

- Encryption: Coding and scrambling of messages to prevent their access without authorization
- Authentication: Ability of each party in a transaction to ascertain identity of other party
- Message integrity: Ability to ascertain that transmitted message has not been copied or altered

Security and Electronic Commerce

- Digital signature: Digital code attached to electronically transmitted message to uniquely identify contents and sender
- Digital certificate: Attachment to electronic message to verify the sender and to provide receiver with means to encode reply

Establishing a Framework for Security and Control

- MIS audit
  - Examines firm’s overall security environment as well as controls governing individual information systems
  - Reviews technologies, procedures, documentation, training, and personnel.
  - May even simulate disaster to test response of technology, IS staff, other employees.
  - Lists and ranks all control weaknesses and estimates probability of their occurrence.
  - Assesses financial and organizational impact of each threat

Thank You…